STATEMENT OF THE HONORABLE CLAY JOHNSON III
DEPUTY DIRECTOR FOR MANAGEMENT
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE COMMITTEE ON GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES
June 8, 2006

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me to speak about the adequacy of existing laws, regulations, and policies regarding privacy, information security, and data breach notification.

Unfortunately, I am here today in the wake of an unprecedented security breach causing the loss of personal data concerning millions of people. Clearly we have a problem. Losing any type of government data is bad enough, but losing personal data is especially troubling as it undermines the public's trust and confidence in our ability to protect them as individuals and keep them from harm.

As your invitation requested, I will describe our review of existing laws and policies, the lessons we have learned from the recent incident and steps for improving our response in the future. You will note the steps we are taking include a focus on better understanding how security programs are actually performing to help avoid breaches in the first place.

Over the past several weeks since the incident, we have reexamined the law and policies designed to prevent problems such as this. We have looked for weaknesses in the policies themselves and in our oversight and measurement of agency performance in implementing them. While we believe the law and policies are generally sound and this incident would not have occurred had elementary and long-standing security procedures been followed, this is a hollow victory and we are left with the same unacceptable results – a breach placing the data concerning millions of people at risk and from which each individual may have to recover.

Our review has identified four specific, but related issues. First, the recent incident makes painfully obvious a long-known security risk – a single trusted individual can mistakenly or intentionally and very quickly, undo all of the sophisticated and expensive controls designed to safeguard our information and systems from attack. To safeguard against this risk, the agencies themselves must be held accountable for implementing existing policies such as segregating personnel duties so one person cannot cause such damage.

Second, good security and privacy are shared responsibilities. As you know, within a framework of laws developed by Congress and through direction from the President, the Office of Management and Budget (OMB) develops policies for and oversees agencies' programs to protect security and information privacy. Agencies are responsible for implementing the policies based upon the risk and magnitude of harm that would result from a breach in their security, ensuring their programs are managed to maintain risk at an acceptable level, and Inspectors General must independently evaluate effectiveness. Each individual, from rank and file employees and their supervisors to independent evaluators and overseers, must be held accountable for performing their assigned responsibilities. The American public expects and deserves positive results from all of us.

Third, while we have seen significant improvements in agency security planning – more than 80% of government systems are certified and accredited, 17 Inspectors General rate agency planning processes as satisfactory or better and 12 Inspectors General indicate their agency has put this planning into practice improving their security performance – our view of the state of government security is much the same as reflected in your Committee’s annual security report card – it is not nearly where it must be.

Of course we all know good planning is not enough. Plans must be executed and agency employees must be instructed in clear and unambiguous terms on how to use them, the rules they must go by, and what will happen if the rules are not followed. Equally and perhaps more importantly, managers must oversee execution, ensure their employees are in fact doing what the plans say must be done, and continually monitor operational effectiveness in an ever-changing risk environment. Finally, as the Federal Information Security Management Act says, Inspectors General must independently evaluate their agencies’ programs. To get a better picture of how agencies are executing their plans, I am directing each agency head to describe in their annual Federal Information Security Management Act report the specific actions they take to ensure their plans are in fact being implemented.

Fourth, security and privacy are commonly seen as separate responsibilities and programs. They are not. We see them as separate pieces of the same puzzle – personally identifiable information is an example of what to protect, while security is a program for how to protect it. At least in part due to this program separation, agencies also characterize differently how and when to report incidents and breaches involving privacy and security. There are also differences in how agencies characterize and report incidents and breaches stemming from physical or cyber incidents.

Correcting this problem involves both near and mid-term efforts. We have begun reviewing these issues using both the Identity Theft Task Force established by Executive order on May 10, 2006, and an OMB-led working group of agency privacy experts. Additionally, we will begin working with the Department of Homeland Security, designated by law as the government’s central cyber incident coordination organization, to combine incident reporting. Without prejudging the results of these efforts, we will remove any artificial and unnecessary barriers or differences between various reporting practices for security and privacy incidents, and make clear to all agency employees what they must report, to whom, and within what specific timeframe.

In taking these actions, we will certainly continue to apply our current policy of immediate reporting of the highest-impact incidents such as the recent loss of personally identifiable information. We will also see if revisions are needed to the current reporting requirements and schedules for lower impact incidents. Also, to ensure a more timely picture of all agencies' operational security, I have directed my staff to work with the Department of Homeland Security, the Chief Information Officers Council, and Senior Agency Officials for Privacy to identify the appropriate level of detail and a schedule for distributing periodic incident reports to agency officials.

At my direction, Senior Agency Officials for Privacy are now reviewing the effectiveness of their security programs and will report to OMB their findings early this fall with their agency's annual reports under the Federal Information Security Management Act. These reports will help us identify the extent to which additional actions are necessary.

I also would like to mention longer-term steps we are taking to increase the security of our sensitive information, computer systems, facilities, and employees. In response to an August of 2004 Presidential directive, OMB led the development of a common identification standard for several million Federal employees and contractors. This directive requires all Executive branch agencies to conduct background checks on their employees and contractors before issuing them permanent government identification. The agencies are now conducting these checks and in October of this year, will begin issuing new identification cards. These cards have built-in security features to control access to government computer systems and the government's physical facilities.

I have outlined above a number of actions we are taking to demonstrate the Administration takes its information privacy and security responsibilities very seriously. These will help prevent a recurrence of an incident such as we just experienced, permit us to better respond if prevention fails, and provide us a more complete and timely view of the security performance of the agencies. Agencies spend more than $4.5 billion each year on controls to protect information and computer systems and we will use the budget process to ensure this money is wisely spent and re-emphasize new spending on information technology will not be approved if sound security is not already in place for existing systems and programs. We are prepared to take more action as necessary and I look forward to working with you to improve our security and privacy programs and welcome any suggestions you have.